(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年11 月10 日 (10.11.2005)

PCT

(10) 国際公開番号
WO 2005/107139 A1

(51) 国際特許分類[7]: H04L 9/08

(21) 国際出願番号: PCT/JP2005/007894

(22) 国際出願日: 2005 年4 月26 日 (26.04.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-133100 2004 年4 月28 日 (28.04.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 村上 隆史 (MURAKAMI, Takashi). 新谷 保之 (SHINTANI, Yasuyuki).

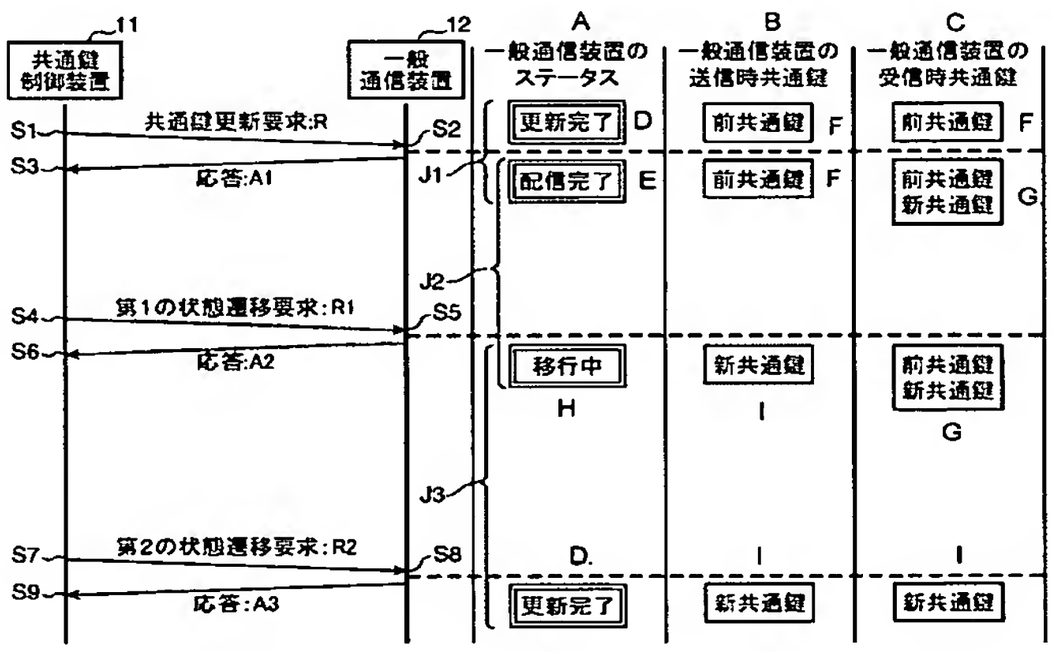
(74) 代理人: 小谷 悦司，外(KOTANI, Etsuji et al.); 〒5300005 大阪府大阪市北区中之島２丁目２番２号ニチメンビル２階 Osaka (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD,

[続葉有]

(54) Title: COMMUNICATION SYSTEM, COMMON KEY CONTROL APPARATUS, AND GENERAL COMMUNICATION APPARATUS

(54) 発明の名称: 通信システム、共通鍵制御装置、及び一般通信装置



11... COMMON KEY CONTROL APPARATUS
R... REQUEST COMMON KEY UPDATE
A1... RESPOND
R1... REQUEST FIRST STATUS TRANSITION
A2... RESPOND
R2... REQUEST SECOND STATUS TRANSITION
A3... RESPOND
12.. GENERAL COMMUNICATION APPARATUS
A... STATUS OF GENERAL COMMUNICATION APPARATUS
D... UPDATE COMPLETION
E... DISTRIBUTION COMPLETION
H... TRANSITION
B... COMMON KEY OF GENERAL COMMUNICATION APPARATUS DURING TRANSMISSION
F... PREVIOUS COMMON KEY
I... NEW COMMON KEY
C... COMMON KEY OF GENERAL COMMUNICATION APPARATUS DURING RECEPTION
G... PREVIOUS AND NEW COMMON KEYS

(57) **Abstract:** To reduce memory consumption amount of a general communication apparatus when a common key is updated by use of a new common key, and further prevent occurrence of an interval for which none of general communication apparatuses become unable to communicate with each other by use of encrypted data. When the statuses of all of the general communication apparatuses (12) become a distribution completion, a common key control apparatus (11) transmits a first status transition request (R1) to all of the general communication apparatuses. When the statuses of all of the general communication apparatuses (12) become transition, the common key control apparatus (11) transmits a second status transition request (R2) to all of the general communication apparatuses. When receiving a new common key from the common key control apparatus (11), a general communication apparatus (12) shifts its status from an update completion to the distribution completion. When receiving the first status transition request, the general communication apparatus (12) shifts its status from the distribution completion to the transition. When receiving the second status transition request, the general communication apparatus (12) returns its status from the transition to the update completion.

(57) 要約: 共通鍵を新しい共通鍵で更新する際に、一般通信装置のメモリ消費量を抑制しつつ、全ての一般通信装置間で暗号化したデータを用いて相互に通

[続葉有]

WO 2005/107139 A1

SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

信することができなくなる期間の発生を防止する。　共通鍵制御装置１１は、全ての一般通信装置１２のステータスが配信完了になったとき、全ての一般通信装置に第１の状態遷移要求Ｒ１を送信し、全ての一般通信装置１２のステータスが移行中になったとき、全ての一般通信装置に第２の状態遷移要求Ｒ２を送信する。一般通信装置１２は、共通鍵制御装置１１から新共通鍵を受信したとき、ステータスを更新完了から前記配信完了に遷移させ、前記第１の状態遷移要求を受信したとき、ステータスを前記配信完了から前記移行中に遷移させ、前記第２の状態遷移要求を受信したとき、ステータスを前記移行中から更新完了に戻す。